

UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of:

INFORMATION ASSOCIATED WITH APPLE ICLOUD  
USEARNAME shakey\_davis@icloud.com STORED BY  
PREMISES CONTROLLED BY APPLE, INC. OF  
CUPERTINO PARK, CALIFORNIA

Case No. 18-M-1316

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

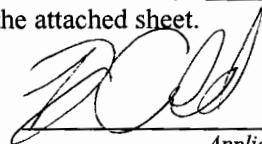
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18 U.S.C. § 371, Title 18 U.S.C. § 922(a)(6), Title 18 U.S.C. § 922(g), Title 18 U.S.C. § 922(d)(9), Title 18 U.S.C. § 922(a)(6), and/or Title 21 U.S.C. § 841(a)(1)

The application is based on these facts: See attached affidavit.

- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



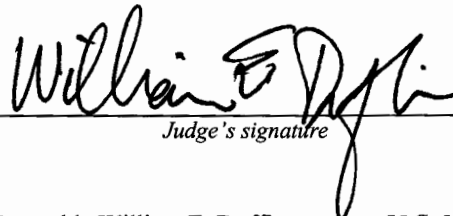
Applicant's signature

Special Agent Ryan Arnold, ATF

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 10/22/18



Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Duffin

, U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Ryan Arnold, being first duly sworn, hereby depose and state as follows:

**I. INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Apple iCloud address that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., which is a provider of electronic communications services or remote computing services in Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple, Inc., disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the iCloud account. It is believed that the information associated with iCloud account shakey\_davis@icloud.com may contain evidence of violations of 18 U.S.C. 371 (conspiracy to sell or transfer firearms to prohibited persons), 18 U.S.C. 922(a)(6) (any person in acquisition of any firearm knowingly furnish a false written or oral statement intended to deceive the dealer), 18 U.S.C. Section 922(g) (possession of firearm by a prohibited person, drug user), 18 U.S.C. 922(d)(9) (sale or transfer of firearm to a prohibited person), 18 U.S.C. 922(a)(6) (false statement as to material fact to FFL), and/or 21 U.S.C. 841(a)(1) (manufacture, dispense, disperse a controlled substance). As a result, a request is submitted for a search warrant to review information associated with the

aforementioned Apple iCloud address. The information to be searched is described in the following paragraphs and in Attachment A.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been since April 2015. As an ATF Special Agent, I have participated in numerous investigations regarding the unlawful possession of firearms by convicted felons. I have also conducted investigations related to the unlawful use of firearms, firearms trafficking, drug trafficking, and arson.

3. Prior to my employment with ATF, I was a Special Agent with the United States Secret Service (USSS) for nearly 5 years. My duties included providing and planning dignitary protection, drafting and executing Federal search warrants, investigations of organized crime networks, investigations of threats against USSS protectees, fraud networks, counterfeit currency investigations, and other financial crime investigations.

4. Previous to my tenure with the USSS, I served as a police officer with the Chicago, Illinois, Police Department (CPD). During part of my career as a CPD Officer, I was assigned to the Organized Crime Division-Gang Enforcement Unit. My responsibilities included the investigations of street gangs, narcotics distribution, firearms violations, robbery, home invasions, operating in an undercover capacity, and the authoring and execution of search warrants.

5. Furthermore, Your Affiant knows from training and experience it is common for drug users, drug dealers, firearms traffickers, and firearms straw

purchasers to communicate via cellular phone through a variety of electronic media. It also common for firearm traffickers and straw buyers to communicate through cellular phones and electronic media. Many times drug dealers also act as firearms traffickers by utilizing the non-prohibited status (no felony convictions) of drug users to obtain firearms. In turn, these firearms are used by the drug trafficking organization to protect and secure their goods and territory. The participants in these organizations can use text (SMS) messaging, iMessage, phone calls, electronic mail, messaging applications, and various social media applications such as Facebook, Snapchat, or Twitter.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

## **II. PURPOSE OF THIS AFFIDAVIT**

7. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to requiring Apple Inc. ("Apple") to disclose records and other information, including the contents of communications, associated with the Apple ID shakey\_davis@icloud.com, stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, California. The warrant I seek would also authorize the government

to search the information described below and in Attachment A for the things described in Attachment B.

8. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

9. The Apple iCloud account, shakey\_davis@icloud.com, belonging to Shakie Davis, AKA Shakey Davis, AKA Shakebag, herein described as a personal website that is accessed with a username and password specific only to that page, has the capability to store and backup information from Apple products, and further described in Attachment A.

10. The applied-for warrant would authorize the search and recovery of evidence particularly described in Attachment B.

### **III. PROBABLE CAUSE**

11. In spring 2017, the ATF identified suspicious firearm purchases that originated in Fond du Lac, Wisconsin, but the firearms were recovered in criminal activity in Chicago, Illinois.

12. Through firearm purchase records, ATF identified that Justin Norton purchased eleven firearms in 2016 from Mill's Fleet Farm and Midwestern Shooter's Supply, both Federal Firearm Licensees (FFLs) located in the Fond du Lac area. Norton attempted to purchase a twelfth firearm in 2016, but the sale was denied. For each firearm, Norton completed the ATF Firearm Transaction Form 4473, and he claimed to

be the actual buyer of the firearms when he answered "YES" in response to question No. 11(a), which asked if he was the actual buyer of the firearms when, in fact, as Norton knew, he was acquiring the firearms for others.

13. In April 2018, ATF interviewed Norton who stated that he had been a heroin addict between 2011 and 2017. Norton stated that Jonathan Griffin, Treon Dennis, Jason Spinks, and Shakie Davis were heroin dealers in Fond du Lac who supplied him with heroin between April 2016 - April 2017. Norton stated that in August 2016, he began to purchase firearms for Griffin, Spinks, and Dennis, frequently in exchange for heroin. Norton stated that Griffin told him that he would obliterate the serial numbers from firearms, and on one occasion, Griffin showed Norton a firearm purchased by Norton that had the serial number removed. Norton stated that Shakie Davis would, at times, coordinate the illegal transfer of firearms.

Justin Norton Firearm Purchases for Jonathan Griffin

14. Norton explained that he purchased nine firearms for Griffin, typically in exchange for approximately .5 grams of heroin. Norton also stated that he attempted to buy a tenth firearm for Griffin, but the sale was denied. In November 2017, Griffin's associate, Dimitrius Phipps, told ATF agents that on November 9, 2016, he was present for one of those transactions when Norton gave Griffin a Century Arms, .223 caliber firearm, and Griffin gave Norton money for the purchase. Table 1 shows Norton's nine firearm purchases and one attempted purchase for Griffin.



**TABLE 1: NORTON'S FIREARM PURCHASES FOR GRIFFIN**

| <b>Firearm</b>  | <b>False Statement Date and Location</b>               | <b>Recovery Date and Location</b> |
|---|--|-----------------------------------|
| Taurus, 9mm with serial number TJN05275                   | 4/26/16<br>Mill's Fleet Farm                           | Unknown                           |
| Taurus, 9mm with serial number TJN98875                   | 4/27/16<br>Mill's Fleet Farm                           | Unknown                           |
| Glock, .45 caliber with serial number MRR251              | 6/10/16<br>Midwestern Shooter's Supply                 | Unknown                           |
| Smith & Wesson, .40 caliber with serial number FXT4223    | 8/16/16<br>Mill's Fleet Farm                           | 12/13/16<br>Chicago               |
| Springfield, 9mm with serial number XD824759              | 8/25/16<br>Midwestern Shooter's Supply                 | 10/17/16<br>Chicago               |
| Ruger, 9mm with serial number 335-73237                   | 9/10/16<br>Midwestern Shooter's Supply                 | 7/3/17<br>Chicago                 |
| Sig Sauer, 9mm with serial number EAK124377               | 10/18/16<br>Midwestern Shooter's Supply                | Unknown                           |
| Century Arms, .223 caliber with serial number M85PV005777 | 11/9/16<br>Mill's Fleet Farm                           | Unknown                           |
| Magnum Research, .40 caliber with serial number PB 100016 | 11/10/16<br>Midwestern Shooter's Supply                | Unknown                           |
| Smith & Wesson, .45 caliber with serial number SHH2043    | SALE DENIED<br>12/13/16<br>Midwestern Shooter's Supply | NA                                |

Justin Norton Firearm Purchase for Jason Spinks

15. On May 12, 2016, Spinks made the following post on his Facebook account, "Made My Mind Up I'm Treatin Myself To The Glizzy 23🤔😞😏😏 No #Pressure jus #Heat👌." Affiant knows from training and experience that "Glizzy" is

slang for Glock, and in this instance a "Glizzy 23" means a Glock, model 23, .40 caliber pistol. Norton stated that Spinks told him to purchase a Glock pistol.

16. On May 14, 2016, Norton went to Midwestern Shooter's Supply and purchased a Glock pistol, model 23, .40 caliber pistol with serial number BBTE120. Following the transfer, Norton provided this firearm to Spinks. Norton did not receive payment for this firearm. On February 22, 2017, Spinks was arrested in Chicago while in possession of the Glock with serial number BBTE120. Ballistic testing confirmed that the firearm was used in two shootings in Chicago on June 30, 2016 and November 3, 2016. **Table 2** shows Norton's firearm purchase for Spinks.

**TABLE 2: NORTON'S FIREARM PURCHASE FOR SPINKS**

| Firearm                                       | False Statement Date and Location      | Recovery Date and Location |
|---|--|----------------------------|
| Glock, .40 caliber with serial number BBTE120 | 5/14/16<br>Midwestern Shooter's Supply | 2/12/17<br>Chicago         |

*Justin Norton Firearm Purchase for Treon Dennis*

17. On August 28, 2016, Treon Dennis contacted Norton to purchase a firearm in exchange for heroin. Norton went to Midwestern Shooter's Supply and purchased a Bersa, 9mm firearm with serial number F31669. Norton explained that Dennis and he went to the store together, at which time, Dennis gave him the money to purchase the firearm. After Norton gave the firearm to Dennis, Dennis gave Norton approximately one gram of heroin as payment. During an August 28, 2016, Facebook conversation between Dennis and Spinks, Dennis posted a photograph of the firearm with a visible



serial number. Lastly, Dennis made a statement to ATF confirming that Norton purchased the firearm for him in exchange for heroin, and that Dennis eventually transferred that firearm to Spinks. **Table 3** shows Norton's one firearm purchase for Dennis.

**TABLE 3: NORTON'S FIREARM PURCHASE FOR DENNIS**

| <b>Firearm</b>                       | <b>False Statement Date and Location</b> | <b>Recovery Date and Location</b> |
|--------------------------------------|--|-----------------------------------|
| Bersa, 9mm with serial number F31669 | 8/28/16<br>Midwestern Shooter's Supply   | Unknown                           |

**SHAKIE DAVIS' ARREST, CELLPHONES, AND CONVICTION**

18. On April 12, 2017, the Fond du Lac Police Department (FDLPD) arrested Shakie Davis and obtained a state search warrant to search the contents of Shakie Davis' two cellphones. FDLPD informed ATF that they observed the telephone number 920-204-8175 in each of Davis' cellphones. This is the same telephone number that Justin Norton listed on an ATF Form 4473 during a firearm transfer. Davis was charged in Fond Du Lac County, and on July 17, 2017, Davis was convicted for Possession with Intent to Deliver Heroin (>10-50g).

**FACEBOOK EVIDENCE FOR SHAKIE DAVIS**

19. Affiant observed conversations between "Shakey Davis", URL: <https://www.facebook.com/shakey.davis>, Facebook ID No. 100000130434744 and what appears to be Jonathan Griffin's Facebook page. Affiant was able to identify "Shakey Davis" as Shakie L. Davis (DOB: 11/15/1994) by comparing FDLPD photographs of

Davis with the Facebook photographs of "Shakey Davis." Griffin and Davis had numerous communications regarding firearms and illegal drugs. Davis is prohibited from owning firearms for the following convictions: Possession Controlled Substance, Illinois State Statute 720 ILCS 570.0/402-C IL (Convicted: 04/10/2012), Aggravated Battery (Peace Officer), and Illinois State Statute 720 ILCS 5.0/12-3.05-D-4 IL (Convicted: 3/24/2015).

20. The following is a summarization of some communications between Griffin and Davis on Facebook:

10/22/2016:

- GRIFFIN: Bring sum lean bac
- DAVIS: Who got it
- GRIFFIN: Ion know
- DAVIS: Chrisett bd be having it
- GRIFFIN: Dude dats fu shit

21. Affiant knows from training and experience that "lean" is street terminology for the prescription drug, codeine promethazine.

11/12/2016:

- DAVIS: I'm in the funeral it was a link saying that the Feds teaming up wit the police weekend n running in cribs in that they already got some assault riffles out of mfer cribs earlier dis week n dis morning wen I was buying some weed from one of my homies on hoodrich n he

told me dey ran in onna dat cribs today

- GRIFFIN: As I seen that I already know

22. Affiant knows that "weed" is slang for marijuana.

11/30/2016:

- DAVIS: U up bitch let's get high
- GRIFFIN: Come on im already smokin on TT
- DAVIS: bet

12/09/2016:

- DAVIS: ☺☺ GOT THE PACK ON THE PULL UP

23. Affiant knows that "pack" can be street slang for a quantity of illegal drugs used as a source for distribution to illegal drug customers. It can be referring to cocaine or heroin.

01/10/2017:

- DAVIS sends a photograph to GRIFFIN of an object consistent with a semi-automatic pistol
- DAVIS sends a photograph consistent with a Ruger .22 caliber pistol

01/11/2017:

- GRIFFIN sends a photograph of an object consistent with a semi-automatic pistol, a loaded magazine, and a box of ammunition with a "Winchester" label

## APPLE ICLOUD EVIDENCE FOR SHAKIE DAVIS

24. Affiant reviewed the forensic reports generated by FDLPD for two cellphones that are believed to belong to Shakie Davis (described above). Your affiant reviewed the forensic results for the Apple iPhone and observed several conversations that listed shakey\_davis@icloud.com as a participant to the conversation.

25. Affiant observed communications consistent with illegal drug sales on an iMessage chat between shakey\_davis@icloud.com, telephone number 920-251-9678, and telephone number 920-376-6717 (Trey P). Affiant knows from this investigation that Davis used "P" after a name to denote that the person was a drug customer. Additionally, Affiant knows from training and experience that "hav" or "have" is shorthand slang for obtaining illegal drugs; the term "boy" or "boi" is slang for heroin; and the term "girl" is slang for cocaine. The following is summarization of conversations consistent with illegal drug dealing:

### 03/10/2017:

- DAVIS: Watchu need I got girl 2
- Trey P: Hav boy
- Trep P: Sry if its to late
- Trey P: Can I come thru

### 03/24/2017:

- DAVIS: Meet me at little Cesar's on Scott n main
- Trey P: I only got 50 can u do me a favor today

- Trey P: Boi
- Trey P: Can u do that
- DAVIS: Can't do it

26. Affiant observed communications consistent with illegal drug sales on an iMessage chat between shakey\_davis@icloud.com, telephone number 920-251-9678, and telephone number 1-920-273-9285. Affiant knows from training and experience that "bin" or "bindle" is commonly used to refer to .10 grams of heroin; a "half" is 0.5 grams of heroin; a "whole" is 1.0 grams of heroin; and "you good" is a common way for drug customers to ask their drug dealer if they have available product. The following is a summarization of the conversation:

01/19/2017:

- 19202739285: Hey it's Gloria. You have me that ride from meeches that one time. Are you fuckin around with that still?
- DAVIS: Yup wassup?
- 19202739285: Do you do bins?
- DAVIS: Nope. Halfs n wholes

01/21/2017:

- 19202739285: Hey do you still have that white stuff
- 19202739285: 19202739285
- DAVIS: I'm the morning



01/22/2017:

- 19202739285: Hey you good
- DAVIS: On what
- 19202739285: Boi
- DAVIS: Not till the morning

01/23/2017:

- 19202739285: Are you good
- DAVIS: Only girl right now till later

01/25/2017:

- 19202739285: You good
- DAVIS: Yea what u tryna do
- 19202739285: You got boi? Or just girl
- DAVIS: Both
- 19202739285: Okay I'm gonna need boi
- 19202739285: How much? 70 or 75?
- DAVIS: 75 Way
- 19202739285: My house. Did you wanna meet somewhere?
- 19202739285: Should I leave now
- 19202739285: To go to speedway
- DAVIS: Yea

01/30/2017:

- 19202739285: Are you good?
- DAVIS: What yu tryna do
- 19202739285: Another half, I get done with work in 45 minutes so  
can meet up at my house then
- DAVIS: Half of what inn u gotta come to me
- 19202739285: Okay I can do that and of boi
- 19202739285: Is that okay?
- DAVIS: No u can meet me sumwhere that I want to meet n how  
long now
- 19202739285: Okay and I'm on my way home now to grab money  
and then I can meet you wherever. But you have boi still right?
- 19202739285: How long until you're here?
- DAVIS: 2 muns

01/31/2017:

- 19202739285: Can I get a half of boi
- DAVIS: Be dere in 2 mins

02/01/2017:

- 19202739285: Half of boi please, I'm at my sisters again like  
yesterday

- DAVIS: U gotta cum to me car in shop till later or wait till 2 till wen my girl get off work
- 19202739285: Sorry about that my message didn't go through to you. But I'm at my house
- DAVIS: I gave you 80 again instead of 75 because I figured she didn't have any change or you did. So next time I'll do 70 & you can just keep the other five because I feel bad for my message not going through earlier. :)
- DAVIS: Okay

02/09/2017:

- 19202739285: You good?
- DAVIS: Yea wassup what u tryna do
- 19202739285: A half
- 19202739285: I can come to you
- 19202739285: Omw to you
- DAVIS: Ok
- 19202739285: Hey I weighed my bag up because it looked short and it said it was .39 instead of .5- so idk if your scales off or what. Also you forgot to give me change but that extra 5 will just go towards my next bag :)
- 19202739285: Just wanted to let you know,

- DAVIS: Okay n going to look out for u on the next one gotta check my scale cause dey did look shorty

04/11/2017:

- DAVIS: Wat u tryna do
- 19202739285: A gram
- 19202739285: I have to be at work at 4 so do you think we could do this before then
- DAVIS: Yea
- DAVIS: Meet me at menard in 20 min
- 19202739285: Ok

27. The above messages suggest that Davis utilized Apple products to conduct illegal activities. Furthermore, the cellphone forensics suggest that some of these activities were memorialized and stored on Apple iCloud.

#### **APPLE ICLOUD INFORMATION GENERALLY**

28. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant

messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be used through numerous iCloud-connected services and can store iOS device backups and data associated with third-party apps.
  - d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share images and videos with other Apple subscribers.
  - e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.
  - f. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers.
29. Apple services are accessed through an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services.
30. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address or an email address associated with a third-party email provider. The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID.



31. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account, the methods used to connect to and utilize the account, the Internet Protocol ("IP") address used to register and access the account, and other log files that reflect usage of the account.

32. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

33. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains

the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service.

34. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party

apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can be decrypted by Apple.

35. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. For example, stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity. In this case in particular, it appears that Shakie Davis used his Apple ID of shakey\_davis@icloud.com to conduct illegal drug sales, and those illegal drug sales may be connected to illegal firearm transactions.

36. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every

device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account.

#### **IV. CONCLUSION**

37. Based on the foregoing, I request that the Court issue the prosoed search warrant.

38. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court of the Eastern District of WI is a district court of the United States that has jurisdiction over the offense(s) being investigated, 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

## **ATTACHMENT A**

### **Property to Be Searched**

This warrant applies to information associated with shakey\_davis@icloud.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.



## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Apple**

To the extent that the information is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for the account listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

- c. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;
- d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);
- f. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;
- g. All records pertaining to the types of service used;
- h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

## **II. Information to be seized by the government.**

All information described above in Section I that constitutes evidence or instrumentalities of violations of may contain evidence of violations of 18 U.S.C. 371 (conspiracy to sell or transfer firearms to prohibited persons), 18 U.S.C. 922(a)(6) (any person in acquisition of any firearm knowingly furnish a false written or oral statement intended to deceive the dealer), 18 U.S.C. Section 922(g) (possession of firearm by a prohibited person, drug user), 18 U.S.C. 922(d)(9) (sale or transfer of firearm to a prohibited person), 18 U.S.C. 922(a)(6) (false statement as to material fact to FFL), and/or 21 U.S.C. 841(a)(1) (manufacture, dispense, disperse a controlled substance), from 2016 to the present, including:

- a. All information and communications in any form, including text messages, instant messages, emails, and other forms of messages concerning the transfer, coordination of transfers, and/or sale of firearms, narcotics, or ammunition;
- b. Photographs or videos of firearms, narcotics, or ammunition;
- c. All call and messaging logs;
- d. Contact lists, to assist with the interpretation of the communications documented in the call logs and to identify the parties listed as affiliated with firearms, narcotics, or ammunition;
- e. Evidence of user attribution, showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, notes, documents and Internet browsing history;
- f. Evidence of use of third-party apps and websites, such as Facebook, related to the offenses under investigation;

- g. The identity and location of the persons who have used the Apple ID;
- h. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- i. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information); and
- j. Evidence that may identify any co-conspirators, aiders and abettors, or customers including records that help reveal their whereabouts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.